References

Module 01: Introduction to Penetration Testing and Methodologies

1. Ethical Hacking vs. Penetration Testing, last modified: 2016, http://resources.infosecinstitute.com/ethical-hacking-vs-penetration-testing/#gref.
2. Neil Roiter, 10 tips for a successful penetration testing program, last modified: 2010, https://www.csoonline.com/article/2126101/access-control/10-tips-for-a-successful-penetration-testing-program.html.
3. Chad Horton, Types of Penetration Testing: The What, The Why, and The How, accessed: January 5, 2018, http://blog.securitymetrics.com/2016/12/types-of-penetration-testing-what-why-how.html.
4. Chad Horton, Different Types of Penetration Tests for Your Business Needs, accessed: January 5, 2018, http://blog.securitymetrics.com/2017/01/what-types-of-penetration-tests-you-need.html.
5. Understanding the Different Types of Penetration Tests, accessed: January 5, 2018, https://www.intelisecure.com/security-assessments-pen-testing/types-of-tests/.
6. Penetration Testing Benefits, last modified: 2017, http://resources.infosecinstitute.com/penetration-testing-benefits/#gref.
7. SEYMOUR BOSWORTH, M.E. KABAY and ERIC WHYNE, COMPUTER SECURITY HANDBOOK, last modified: 2009, http://www.mekabay.com/overviews/csh5_fm.pdf.
8. Farkhod Alisherov A., and Feruza Sattarova Y, Methodology for Penetration Testing, last modified: 2009, http://www.sersc.org/journals/IJGDC/vol2_no2/5.pdf.
9. Penetration Testing Methodology, accessed: January 5, 2018, http://www.syrinxtech.com/uploads/1/2/8/1/12815379/penetration_testing_methodology.pdf.
10. Karen Scarfone (NIST), Murugiah Souppaya (NIST), Amanda Cody (BAH), Angela Orebaugh (BAH), Technical Guide to Information Security Testing and Assessment, last modified: 2008, http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf.
11. Debasis Mohanty, Demystifying Penetration Testing, accessed: January 5, 2018, http://www.infosecwriters.com/text_resources/pdf/pen_test2.pdf.
12. Integrated Network Vulnerability Scanning and Penetration Testing, last modified: 2009, http://www.saintcorporation.com/resources/SAINT_integrated_pen_testing.pdf.
13. Automated Penetration Testing; Can IT Afford Not To?, last modified: 2007, https://www.bitpipe.com/detail/RES/1120073352_152.html.
14. Penetration Testing, accessed: January 5, 2018, http://www.penetration-testing.com.
15. Performing a penetration test, accessed: January 5, 2018, http://searchnetworking.techtarget.com/tutorial/Performing-a-penetration-test.
16. Dr. Daniel Geer and John Harthorne, Penetration Testing: A Duet, accessed: January 5, 2018, http://www.acsac.org/2002/papers/geer.pdf.
17. Penetration testing strategies, accessed: January 5, 2018, http://searchnetworking.techtarget.com/tutorial/Penetration-testing-strategies.
18. Ron Gula, BROADENING THE SCOPE OF PENETRATION-TESTING TECHNIQUES, last modified: 1999, http://www.forum-intrusion.com/archive/ENTRASYS.pdf.
19. Arian Eigen Heald, Understanding Security Testing, accessed: January 5, 2018, http://www.infosecwriters.com/text_resources/pdf/Types_of_Security_Testing.pdf.
20. Pen-Testing Process, accessed: January 5, 2018, http://www.mhprofessional.com/downloads/products/0072257091/0072257091_ch04.pdf.
21. Sara Kraemer, Pascale Carayon and Ruth Duggan, RED TEAM PERFORMANCE FOR IMPROVED COMPUTER SECURITY, http://cis.engr.wisc.edu/docs/skhfes2004.pdf.
22. Toggmeister (a.k.a Kev Orrey) and Lee J Lawson, Penetration Testing Framework v0.21, http://www.infosecwriters.com/text_resources/pdf/PenTest_Toggmeister.pdf.
23. Gray box testing, accessed: January 5, 2018, http://en.wikipedia.org/wiki/Gray_box_testing#White_box.2C_black_box.2C_and_grey_box_testing.

24. Types of penetration tests, accessed: January 5, 2018, http://searchnetworking.techtarget.com/tutorial/Types-of-penetration-tests.

25. Penetration Testing, accessed: January 5, 2018, http://www.fma-rms.com/services/remotenetworkpenetrationtesting.php.

26. War Dialing, accessed: January 5, 2018, http://www.tech-faq.com/war-dialing.html.

27. Abhishek Singh, Demystifying Denial-Of-Service attacks, part one, last modified: 2005, http://www.symantec.com/connect/articles/demystifying-denial-service-attacks-part-one.

28. What is Penetration Test?, accessed: January 5, 2018, http://www.secpoint.com/what-is-penetration-testing.html.

29. Manish S. Saindane, PENETRATION TESTING – A SYSTEMATIC APPROACH, accessed: January 5, 2018, http://www.infosecwriters.com/text_resources/pdf/PenTest_MSaindane.pdf.

30. Marcia Wilson, Demonstrating ROI for Penetration Testing (Part One), last modified: 2003, https://www.pcisecuritystandards.org/documents/Penetration_Testing_Guidance_March_2015.pdf.

31. Information Supplement: Penetration Testing Guidance, last modified: 2015, .

32. Jason Creasey, A guide for running an effective Penetration Testing programme, last modified: 2017, https://www.crest-approved.org/wp-content/uploads/CREST-Penetration-Testing-Guide.pdf.

33. A Penetration Testing Model, accessed: January 5, 2018, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Studies/Penetration/penetration_pdf.pdf?__blob=publicationFile.

34. The Penetration Testing Execution Standard Documentation Release 1.1, last modified: 2017, https://media.readthedocs.org/pdf/pentest-standard/latest/pentest-standard.pdf.

35. Georgia Weidman, Penetration Testing - A hands-on introduction to Hacking, last modified: 2014, https://repo.zenk-security.com/Magazine%20E-book/Penetration%20Testing%20-%20A%20hands-on%20introduction%20to%20Hacking.pdf.

36. Patrick Engebretson, The Basics of Hacking and Penetration Testing, last modified: 2011, https://doc.lagout.org/security/Syngress.The.Basics.of.Hacking.and.Penetration.Testing.Aug.2011.pdf.

37. SECURITY FIRST: AN ESSENTIAL GUIDE TO PENETRATION TESTING, accessed: January 5, 2018, https://www.ipexpoeurope.com/content/download/7535/100772/file/ServerChoice%20-%20Penetration%20Testing%20White%20Paper%20(web).pdf.

38. Penetration Testing Methodology, accessed: January 5, 2018, http://www.syrinxtech.com/uploads/1/2/8/1/12815379/penetration_testing_methodology.pdf.

39. Penetration Test, accessed: January 5, 2018, https://www.secneo.com/public/uploads/whitepaper/penetrationtest.pdf.

40. Andrew Whitaker, Denial P.Newman, Penetration Testing and Network Defense, last modified: 2005, http://ebook.eqbal.ac.ir/Security/Penetration%20Testing/Network/Penetration%20Testing%20and%20Network%20Defense.pdf.

Module 02: Penetration Testing Scoping and Engagement

41. Farkhod Alisherovich Alisherov, Considerations for Penetration Testing Policy Establishment, last modified: 2008, http://www.sersc.org/journals/JSE/vol5_no5_2008/10.pdf.

42. VA Privacy and Information Security Awareness and Rules of Behavior, accessed: January 8, 2018, http://www.wichita.va.gov/documents/Privacy-and-Information-Security-Awareness-and-Rules-of-Behavior_121012.pdf.

43. GENERATING VALUE WITH CONTINUOUS SECURITY TESTING AND MEASUREMENT, accessed: January 8, 2018, https://telecomtest.com.au/datasheet/Spire-Continuous-Security-Testing-ROI.pdf.

44. Penetration Testing Agreement, accessed: January 8, 2018, https://itsecurity.uiowa.edu/sites/itsecurity.uiowa.edu/files/wysiwyg_uploads/penetrationtestingagreement.pdf.

45. Non-disclosure agreements, last modified: 2015, https://www.gov.uk/government/publications/non-disclosure-agreements.

46. CONFIDENTIALITY AGREEMENT, accessed: January 8, 2018, https://www.coollawyer.com/free-confidentiality-agreement-free-nda.html.

47. RULES OF BEHAVIOR, last modified: 2006, https://workforcesecurity.doleta.gov/dv/pdf/rules_of_behavior.pdf.

48. Amit Singh, How to choose your Security / Penetration Testing Vendor?, last modified: 2017, https://www.firecompass.com/blog/choose-penetration-testing-vendor/.

49. Jonathan Trull, Security Through Effective Penetration Testing, last modified: 2012, https://www.isaca.org/Journal/archives/2012/Volume-2/Pages/Security-Through-Effective-Penetration-Testing.aspx.

50. Kevin L.Shaw and Leonard Mansell, Penetration Testing – Scoping, Rules of Engagement, and Basic Techniques, last modified: 2013, https://pdfsecret.com/download/encari-penetration-testing-nerc_59f759d9d64ab20a7517dd38_pdf.

51. Paul D. Robertson, Introduction to Penetration Testing, last modified: 2013, http://www.rcfg.org/gmu/wp-content/uploads/2013/08/GMU-2013-Intro-to-Pentesting-np.pdf.

52. T. Dimkov, Wolter Pieters, Pieter H. Hartel, Two methodologies for physical penetration testing using social engineering, last modified: 2009, http://doc.utwente.nl/69064/1/Pentesting_methodology.pdf.

53. John Verry, What is a NIST Penetration Test?, last modified: 2013, https://www.pivotpointsecurity.com/blog/what-is-a-nist-penetration-test/.

54. RE: rules of engagement scope, last modified: 2006, http://seclists.org/pen-test/2006/May/226.

55. Justin Searle, Utilisec, AMI Penetration Test Plan, accessed: January 8, 2018, https://media.blackhat.com/bh-eu-12/Searle/bh-eu-12-Searle-Smart_Meters-WP.pdf.

56. Limitations of Penetration Testing, last modified: 2018, http://www.pen-tests.com/limitations-of-penetration-testing.html.

57. Rules of Engagement, accessed: January 8, 2018, http://www.pentest-standard.org/index.php/Pre-engagement#Rules_of_Engagement.

58. Karen Scarfone (NIST), Murugiah Souppaya (NIST), Amanda Cody (BAH), Angela Orebaugh (BAH), Technical Guide to Information Security Testing and Assessment, last modified: 2008, http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf.

59. Clark Weissman, Penetration Testing, accessed: January 8, 2018, http://pdf.aminer.org/000/153/109/penetration_testing.pdf.

60. Procedures for IT Security Penetration Testing and Rules of Engagement, accessed: January 8, 2018, http://www.nasa.gov/pdf/368190main_ITS-SOP-0017A%20-%20Procedures%20for%20IT%20Security%20Penetration%20Test%20Plan%20and%20Rules%20of%20Engagement%20(508).pdf.

61. Pentesting IAM & Vulnerability Projects by Core Security, accessed: January 8, 2018, http://corelabs.coresecurity.com/index.php?module=Wiki&action=attachment&type=project&page=Attack_Planning&file=publication%2FSecArt11%2FSecArt11_Sarraute_Buffet_Hoffmann.pdf.

62. CoreLabs Information Security Publications, accessed: January 8, 2018, http://corelabs.coresecurity.com/index.php?module=Wiki&action=attachment&type=publication&page=CORE_IMPACT:_Penetration_Test_Automation&file=CORE_IMPACT-WhitePaper.pdf.

63. T. J. Klevinsky, Scott Laliberte, Ajay Gupta, Hack I.T.: Security Through Penetration Testing, last modified: 2002, https://doc.lagout.org/security/Hack%20IT%20Security%20Through%20Penetration%20Testing.pdf.

64. Ron Gula, BROADENING THE SCOPE OF PENETRATION-TESTING TECHNIQUES, accessed: January 8, 2018, http://www.forum-intrusion.com/archive/ENTRASYS.pdf.

65. TEST PLAN OUTLINE (IEEE 829 FORMAT), accessed: January 8, 2018, https://jmpovedar.files.wordpress.com/2014/03/ieee-829.pdf.

66. Information Supplement: Penetration Testing Guidance, last modified: 2015, https://www.pcisecuritystandards.org/documents/Penetration_Testing_Guidance_March_2015.pdf.

67. The Penetration Testing Execution Standard Documentation Release 1.1, last modified: 2017, https://media.readthedocs.org/pdf/pentest-standard/latest/pentest-standard.pdf.

68. What is Penetration Testing?, accessed: January 8, 2018, http://www.aquion.com.au/sites/default/files/downloads/R7what-is-penetration-testing.pdf.

69. PENETRATION TESTING METHODOLOGIES, last modified: 2014, http://tec.gov.in/pdf/Studypaper/study%20paper%20on%20penetration%20testing_final.pdf.

70. A Penetration Testing Model, accessed: January 8, 2018, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Studies/Penetration/penetration_pdf.pdf?__blob=publicationFile.

71. FedRAMP Penetration Test Guidance, last modified: 2015, https://s3.amazonaws.com/sitesusa/wp-content/uploads/sites/482/2015/01/FedRAMP-PenTest-Guidance-v-1-0.pdf.

Module 03: Open Source Intelligence (OSINT)

72. Chandan Kumar, How to find Subdomains of a Domain in Minutes?, last modified: 2016, https://geekflare.com/find-subdomains/.

73. Shpend Kurtishaj, Discovering Subdomains, last modified: 2016, https://blog.bugcrowd.com/discovering-subdomains.

74. Google Hacking Database (GHDB), accessed: January 9, 2018, https://www.exploit-db.com/google-hacking-database/?action=search&ghdb_search_cat_id=0&ghdb_search_text=voip.

75. Directory of US Associations, accessed: January 9, 2018, http://www.marketingsource.com/directories/associations/us/datasample.

76. Antitrust guidance note Competitive intelligence gathering versus commercially sensitive information exchanges, accessed: January 9, 2018, http://www02.abb.com/global/abbzh/abbzh252.nsf/0/df9558e3445cf87ac12577e900589252/$file/Antitrust+Guidance+Note_Competitive+Intelligence+vs+Commercially+Sensitive+Information.pdf.

77. Christian Martorella, A fresh new look into Information Gathering, accessed: January 9, 2018, http://www.edge-security.com/docs/OWASP-Christian_Martorella-InformationGathering.pdf.

78. Adrian Stoica, A Study on The Inform ation Gathering Method for Penetration Testing, last modified: 2008, http://www.sersc.org/journals/JSE/vol5_no5_2008/6.pdf.

79. Open Source Intelligence Tools and Resources Handbook, last modified: 2016, https://www.i-intelligence.eu/wp-content/uploads/2016/11/2016_November_Open-Source-Intelligence-Tools-and-Resources-Handbook.pdf.

80. OSINT Cheat Sheet, accessed: January 9, 2018, https://www.compass-security.com/fileadmin/Datein/Research/White_Papers/osint_cheat_sheet.pdf.

81. Georgia Weidman, Penetration testing A Hands-On Introduction to Hacking, last modified: 2014, https://repo.zenk-security.com/Magazine%20E-book/Penetration%20Testing%20-%20A%20hands-on%20introduction%20to%20Hacking.pdf.

82. The Penetration Testing Execution Standard Documentation Release 1.1, last modified: 2017, https://media.readthedocs.org/pdf/pentest-standard/latest/pentest-standard.pdf.

83. RAFAY BALOCH, ETHICAL HACKING AND PENETRATION TESTING GUIDE, last modified: 2015, http://www.ittoday.info/Excerpts/Postexploitation.pdf.

84. Open Source Intelligence: A Strategic Enabler of National Security, last modified: 2008, http://www.css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/CSS-Analyses-32.pdf.

85. Get information about a company, accessed: January 9, 2018, https://www.gov.uk/get-information-about-a-company.

86. Andrew Crane, In the company of spies: When competitive intelligence gathering becomes industrial espionage, last modified: 2005, https://www.sciencedirect.com/science/article/pii/S0007681304001302.

87. How can I refine a search query using operators?, accessed: January 9, 2018, https://www.ibm.com/support/knowledgecenter/en/SSKTWP_9.0.0/com.ibm.notes900.help.doc/sch_refine_query_r.html.

88. Whitson Gordon, Top 10 Clever Google Search Tricks, last modified: 2013, https://lifehacker.com/top-10-clever-google-search-tricks-1450186165.

89. Using Advanced Web Search Operators to Find What You're Looking for on the Internet, accessed: January 9, 2018, http://www.datacenter.org/wp-content/uploads/UsingAdvancedGoogleSearchWithOperators.pdf.

90. Google Search Operators – 5 Useful Ways to Refine your Searches in Google, accessed: January 9, 2018, http://www.aillum.com/2014/07/google-search-operators-5-useful-ways-to-refine-your-searches-in-google/.

91. GOOGLE SEARCH CHEAT SHEET, accessed: January 9, 2018, https://supple.com.au/tools/google-advanced-search-operators/.

92. Advanced web search with Google operators, accessed: January 9, 2018, https://www.1and1.com/digitalguide/online-marketing/search-engine-marketing/search-more-effectively-with-google-operators/.

93. David Goldman, Shodan: The scariest search engine on the Internet, last modified: 2013, http://webcache.googleusercontent.com/search?q=cache:http://money.cnn.com/2013/04/08/technology/security/shodan/index.html&gws_rd=cr&dcr=0&ei=QSR4WrmgAsXhvAT6uZf4Aw.

94. Open-source intelligence, accessed: January 9, 2018, https://en.wikipedia.org/wiki/Open-source_intelligence.

95. Riyaz Walikar, Open Source Intelligence Gathering 101, last modified: 2017, https://blog.appsecco.com/open-source-intelligence-gathering-101-d2861d4429e3.

96. Using OSINT sources for penetration testing, accessed: January 9, 2018, https://andreafortuna.org/cybersecurity/information-gathering-tools/.

97. OSINT (Open-Source Intelligence), last modified: 2013, http://resources.infosecinstitute.com/osint-open-source-intelligence/#gref.

98. Gerard Johansen, Lee Allen, Tedi Heriyanto, Shakeel Ali, Kali Linux 2 – Assuring Security by Penetration Testing, last modified: 2016, https://books.google.co.in/books?id=VoFcDgAAQBAJ&pg=PA82&lpg=PA82&dq=osint+information+gathering+in+testing&source=bl&ots=j5kHUmnW_2&sig=PYPE9aSjeZTPMpxDz4p2mBNMa4c&hl=en&sa=X&ved=0ahUKEwjz0snTv47ZAhUFNo8KHUF_By4Q6AEIYzAJ#v=onepage&q=osint%20information%20gathering%20in%20testing&f=false.

99. noor qureshi, OSINT: Information Gathering Tool For Insta, Shodan And Amazon, last modified: 2017, https://thehacktoday.com/osint-information-gathering-tool/.

100. Ali Al-Shemery, Hacking Techniques & Intrusion Detection, accessed: January 9, 2018, http://opensecuritytraining.info/HTID_files/Day05-Recon.pdf.

101. Christian Martorella, A fresh new look into Information Gathering, accessed: January 9, 2018, http://www.edge-security.com/docs/OWASP-Christian_Martorella-InformationGathering.pdf.

102. Open Source Intelligence (OSINT) Threat Management Model, last modified: 2017, https://www.raytheon.com/cyber/rtnwcm/groups/cyber/documents/content/open-source-intelligence.pdf.

103. The Art of Searching for Open Source Intelligence, last modified: 2016, http://resources.infosecinstitute.com/the-art-of-searching-for-open-source-intelligence/#gref.

Module 04: Social Engineering Penetration Testing

104. Chad Horton, Different Types of Penetration Tests for Your Business Needs, accessed: January 5, 2018, http://blog.securitymetrics.com/2017/01/what-types-of-penetration-tests-you-need.html.

105. Screenshots, accessed: January 5, 2018, https://www.phishingfrenzy.com/about/screenshots.

106. Social Engineering, accessed: January 5, 2018, https://www.redspin.com/it-security/penetration-testing/social-engineering/.

107. Christopher J. Hadnagy and James O'Gorman, Social Engineering Capture the Flag Results, last modified: 2011, https://www.social-engineer.com//downloads/Social-Engineer_Defcon_19_SECTF_Results_Report.pdf.

108. Ashish Thapar, Social Engineering, accessed: January 5, 2018, http://www.infosecwriters.com/text_resources/pdf/Social_Engineering_AThapar.pdf.

109. Bernard Oosterloo, Managing Social Engineering Risk, last modified: 2008, http://essay.utwente.nl/59233/1/scriptie_B_Oosterloo.pdf.

110. Matthew J. Warren and Shona Leitch, Social Engineering and its Impact via the Internet, last modified: 2006, http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1081&context=ism.

111. Daniel Franks, Social impact assessment of resource projects, last modified: 2012, http://im4dc.org/wp-content/uploads/2012/01/UWA_1698_Paper-02_Social-impact-assessment-of-resource-projects1.pdf.

112. THE RISK OF SOCIAL ENGINEERING ON INFORMATION SECURITY: A SURVEY OF IT PROFESSIONALS, last modified: 2011, https://www.stamx.net/files/The-Risk-of-Social-Engineering-on-Information-Security.pdf.

113. Thomas Kurian Ambattu, Social Engineering Techniques, accessed: January 5, 2018, http://himis.s3.amazonaws.com/social-engineering-techniques.pdf.

114. M.E. Kabay, Social engineering in penetration testing: Cases, last modified: 2007, http://www.networkworld.com/newsletters/sec/2007/1022sec2.html?page=1.

115. Margaret Rouse, social engineering, accessed: January 5, 2018, http://searchsecurity.techtarget.com/definition/social-engineering.

116. Vishing or Voice Phishing, accessed: January 5, 2018, http://www.rcmp-grc.gc.ca/scams-fraudes/vish-hame-eng.htm.

117. Telemarketing and Unwanted Mail, accessed: January 5, 2018, https://www.usa.gov/telemarketing.

118. What is Social Engineering?, accessed: January 5, 2018, https://www.webroot.com/in/en/home/resources/tips/online-shopping-banking/secure-what-is-social-engineering.

119. Margaret-Anne Storey, Christoph Treude, Arie van Deursen, and Li-Te Cheng, The Impact of Social Media on Software Engineering Practices and Tools, last modified: 2010, http://swerl.tudelft.nl/twiki/pub/Main/TechnicalReports/TUD-SERG-2010-038.pdf.

120. Christopher Hadnagy, Social Engineering:The Art of Human Hacking, last modified: 2011, http://zempirians.com/ebooks/The_Art_of_Human_Hacking.pdf.

121. Danesh Irani, Marco Balduzzi, Davide Balzarotti, Engin Kirda and Calton Pu, Reverse Social Engineering Attacks in Online Social Networks, accessed: January 5, 2018, http://www.syssec-project.eu/m/page-media/3/irani-dimva11.pdf.

122. Shoulder Surfing, accessed: January 5, 2018, https://www.techopedia.com/definition/4103/shoulder-surfing.

123. Shoulder surfing (computer security), accessed: January 5, 2018, https://en.wikipedia.org/wiki/Shoulder_surfing_(computer_security).

124. Richard Ackroyd, The E-mail Attack Vector, last modified: 2014, http://cdn.ttgtmedia.com/rms/security/Social-Engineering-Penetration-Testing-Ch9.pdf.

125. Georgia Weidman, Penetration testing A Hands-On Introduction to Hacking, last modified: 2014, https://repo.zenk-security.com/Magazine%20E-book/Penetration%20Testing%20-%20A%20hands-on%20introduction%20to%20Hacking.pdf.

126. Social Engineering – Risks, Techniques and Safeguards, last modified: 2013, https://www.itegria.com/wp-content/uploads/2014/03/ItegriaSocialEngineering.pdf.

127. Rahul Singh Patel, Kali Linux Social Engineering, last modified: 2013, http://zempirians.com/ebooks/Packt.Kali.Linux.Social.Engineering.Dec.2013.ISBN.1783283270.pdf.

128. Andrew Whitaker, Denial P.Newman, Penetration Testing and Network Defense, last modified: 2006, http://ebook.eqbal.ac.ir/Security/Penetration%20Testing/Network/Penetration%20Testing%20and%20Network%20Defense.pdf.

129. Best Practices for Social Engineering Attacks, accessed: January 5, 2018, https://www.rapid7.com/docs/download/Metasploit_Best_Practices_for_Social_Engineering_Attacks.pdf.

130. Social Engineering Penetration Testing, accessed: January 5, 2018, http://searchsecurity.techtarget.com/feature/Social-Engineering-Penetration-Testing.

131. Joan Goodchild, Social engineering in penetration tests: 6 tips for ethical (and legal) use, last modified: 2013, https://www.csoonline.com/article/2133330/social-engineering/social-engineering-in-penetration-tests-6-tips-for-ethical-and-legal-use.html.

132. The Social Engineering Framework, accessed: January 5, 2018, https://www.social-engineer.org/framework/general-discussion/categories-social-engineers/penetration-testers/.

133. Gavin Watson, Andrew Mason, Richard Ackroyd, Social Engineering Penetration Testing: Executing Social Engineering Pen Tests, Assessments and Defense, last modified: 2014.

134. Nate Lord, SOCIAL ENGINEERING ATTACKS: COMMON TECHNIQUES & HOW TO PREVENT AN ATTACK, accessed: January 5, 2018, https://digitalguardian.com/blog/social-engineering-attacks-common-techniques-how-prevent-attack.

135. OCCUPYTHEWEB, How to Spear Phish with the Social Engineering Toolkit (SET) in BackTrack, last modified: 2013, https://null-byte.wonderhowto.com/how-to/hack-like-pro-spear-phish-with-social-engineering-toolkit-set-backtrack-0148571/.

136. Bill Sweeney, Social Engineering: How an Email Becomes a Cyber Threat, last modified: 2015, http://www.securityweek.com/social-engineering-how-email-becomes-cyber-threat.

137. Tibor Žukina, Social engineering techniques: Vishing, quid pro quo, tailgating, baiting, last modified: 2015, https://sgros-students.blogspot.in/2015/11/social-engineering-techniques-vishing.html.

138. Uladzislau Murashka, Social engineering penetration testing: an overview, last modified: 2018, https://www.scmagazine.com/social-engineering-penetration-testing-an-overview/article/734276/.

139. Ajay Gupta, The Art of Social Engineering, last modified: 2002, http://www.informit.com/articles/article.aspx?p=28802&seqNum=3.

140. Dawn Kuczwara, SOCIAL STUDIES: PENETRATION TESTS FOR YOUR HUMAN NETWORK, last modified: 2016, http://techgenix.com/penetration-testing-human-network/.

141. Social Engineering Review, accessed: January 5, 2018, https://www.canaudit.com/services/it-security-and-it-audit-services/social-engineering-review/.

142. Social Engineering: A Hacking Story, last modified: 2013, http://resources.infosecinstitute.com/social-engineering-a-hacking-story/#gref.

143. D. Dieterle, Social Engineering: Tips to Defend against Shoulder Surfing, last modified: 2010, https://cyberarms.wordpress.com/2010/05/01/social-engineering-tips-to-defend-against-shoulder-surfing/.

144. M.E. Kabay, Social engineering in penetration testing: Cases, last modified: 2007, https://www.networkworld.com/article/2287583/lan-wan/social-engineering-in-penetration-testing--cases.html.

145. Social Engineering, accessed: January 5, 2018, https://www.perspectiverisk.com/our-services/social-engineering/.

146. Phishing is a serious threat to business, accessed: January 5, 2018, https://www.itgovernance.co.uk/phishing-penetration-test.

147. Uladzislau Murashka, (2018), Social engineering penetration testing: an overview, from https://www.scmagazine.com/home/opinion/executive-insight/social-engineering-penetration-testing-an-overview/.

148. Aaron Bond, Social Engineering Penetration Testing: Attacks, Methods, & Steps, from https://purplesec.us/social-engineering-penetration-testing/.

149. Nena Giandomenico, (2019), What is Spear-phishing? Defining and Differentiating Spear-phishing from Phishing, from https://digitalguardian.com/blog/what-is-spear-phishing-defining-and-differentiating-spear-phishing-and-phishing.

150. Spear Phishing, from https://www.imperva.com/learn/application-security/spear-phishing/?.

151. (2020), Whaling: how it works, and what your organisation can do about it, from https://www.ncsc.gov.uk/guidance/whaling-how-it-works-and-what-your-organisation-can-do-about-it.

152. Test Employees, from https://lucysecurity.com/test-employees/.

153. Jeremiah Talamantes, 5 Effective Social Engineering Elicitation Techniques, from https://www.redteamsecure.com/blog/5-effective-social-engineering-elicitation-techniques/.

Module 05: Network Penetration Testing - External

154. Penetration Testing Methodology, accessed: January 5, 2018, http://www.syrinxtech.com/uploads/1/2/8/1/12815379/penetration_testing_methodology.pdf.

155. Karen Scarfone, Murugiah Souppaya, Amanda Cody and Angela Orebaugh, Technical Guide to Information Security Testing and Assessment, last modified: 2008, http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf.

156. T. J. Klevinsky, Scott Laliberte and Ajay Gupta, Hack I.T.: Security Through Penetration Testing, last modified: 2002, https://doc.lagout.org/security/Hack%20IT%20Security%20Through%20Penetration%20Testing.pdf.

157. Network Penetration Testing, accessed: January 10, 2018, https://www.happiestminds.com/whitepapers/Network-Penetration-Testing.pdf.

158. RAFAY BALOCH, ETHICAL HACKING AND PENETRATION TESTING GUIDE, last modified: 2015, http://www.ittoday.info/Excerpts/Postexploitation.pdf.

159. The Types of Penetration Testing, last modified: 2016, http://resources.infosecinstitute.com/the-types-of-penetration-testing/#gref.

160. GURUBARAN S, Network Penetration Testing Checklist, last modified: 2017, 2012.

161. Candice Moschell, Penetration Testing, last modified: 2013, http://www.isaca.org/chapters3/Atlanta/AboutOurChapter/Documents/Penetration%20Testing.pdf.

162. secforce, Black box penetration testing vs white box penetration testing, last modified: 2008, https://www.secforce.com/blog/2008/11/black-box-penetration-testing-vs-white-box-penetration-testing/.

163. Network Penetration Testing, accessed: January 10, 2018, https://paladion.net/network-penetration-testingpen-testing/.

164. Pre-engagement, accessed: January 10, 2018, http://www.pentest-standard.org/index.php/Pre-engagement#General_Questions.

165. Chaitra N. Shivayogimath, AN OVERVIEW OF NETWORK PENETRATION TESTING, last modified: 2014, http://esatjournals.net/ijret/2014v03/i07/IJRET20140307070.pdf.

166. Vulnerability Scanners, last modified: 2016, http://resources.infosecinstitute.com/vulnerability-scanners-2/#gref.

167. EXTERNAL PENETRATION TEST, accessed: January 10, 2018, https://www.hacklabs.com/penetration-testing/.

168. Lee Allen, Advanced Penetration Testing for Highly-Secured Environments:The Ultimate Security Guide, last modified: 2012, https://news.asis.io/sites/default/files/%E2%80%8Cbook.pdf.

169. Aileen G. Bacudio, Xiaohong Yuan, Bei-Tseng Bill Chu, Monique Jones, AN OVERVIEW OF PENETRATION TESTING, last modified: 2011, http://airccse.org/journal/nsa/1111nsa02.pdf.

170. Penetration Tests: A Brief Guide to the Differences between Internal and External Testing, last modified: 2016, http://www.tgdaily.com/security/penetration-tests-a-brief-guide-to-the-differences-between-internal-and-external-testing.

171. John H. Sawyer, Internal vs. External Penetration Testing, last modified: 2008, https://www.darkreading.com/risk/internal-vs-external-penetration-testing/d/d-id/1129881?.

172. Internal vs. External Assessments and Penetration Testing Options, accessed: January 10, 2018, https://www.intelisecure.com/security-assessments-pen-testing/approaches/.

Module 06: Network Penetration Testing - Internal

173. Detecting SSH versions with the SSH version scanner, accessed: January 5, 2018, https://www.packtpub.com/mapt/book/networking_and_servers/9781782166788/2/ch02lvl1sec22/detecting-ssh-versions-with-the-ssh-version-scanner.
174. How to Remotely Grab Encrypted Passwords from a Compromised Computer, last modified: 2016, https://null-byte.wonderhowto.com/how-to/hack-like-pro-remotely-grab-encrypted-passwords-from-compromised-computer-0146655/.
175. Dumping And Cracking Unix Password Hashes, last modified: 2012, https://pentestlab.blog/2012/07/23/dumping-and-cracking-unix-password-hashes/.
176. Keyboard input in Desktop Viewer sessions, last modified: 2013, https://docs.citrix.com/en-us/receiver/windows/4-0/ica-improve-the-user-experience-v2/ica-xd-optimize-keyboards.html.
177. Paul Asadoorian, Linux/UNIX Patch Auditing Using Nessus, last modified: 2013, https://www.tenable.com/blog/linuxunix-patch-auditing-using-nessus.
178. Post Exploitation, accessed: January 5, 2018, http://www.pentest-standard.org/index.php/Post_Exploitation.
179. INTERNAL PENETRATION TEST, accessed: January 5, 2018, https://www.hacklabs.com/internal-penetration-testing.
180. John H. Sawyer, Internal vs. External Penetration Testing, last modified: 2008, https://www.darkreading.com/risk/internal-vs-external-penetration-testing/d/d-id/1129881?.
181. Adam L. Young, Building Robust Backdoors in Secret Symmetric Ciphers, last modified: 2005, http://www.blackhat.com/presentations/bh-usa-05/bh-us-05-young-update.pdf.
182. Get in through the backdoor: Post exploitation with Armitage, accessed: January 5, 2018, http://www.fastandeasyhacking.com/download/postexploitationwitharmitage.pdf.
183. Chris Wysopal, Chris Eng, Static Detection of Application Backdoors, accessed: January 5, 2018, https://www.veracode.com/sites/default/files/Resources/Whitepapers/static-detection-of-backdoors-1.0.pdf.
184. Adam Waksman and Simha Sethumadhavan, Silencing Hardware Backdoors, accessed: January 5, 2018, http://www.cs.columbia.edu/~simha/preprint_oakland11.pdf.
185. Network Penetration Testing, accessed: January 5, 2018, https://www.happiestminds.com/whitepapers/Network-Penetration-Testing.pdf.
186. Penetration Testing Methodology, accessed: January 5, 2018, http://www.syrinxtech.com/uploads/1/2/8/1/12815379/penetration_testing_methodology.pdf.
187. RAFAY BALOCH, ETHICAL HACKING AND PENETRATION TESTING GUIDE, last modified: 2015, http://www.ittoday.info/Excerpts/Postexploitation.pdf.
188. Jarred White, Internal vs. External Vulnerability Scans: Why You Need Both, last modified: 2014, https://www.pcicomplianceguide.org/internal-vs-external-vulnerability-scans-and-why-you-need-both/.
189. Find IP addresses of a private network, accessed: January 5, 2018, https://www.iplocation.net/find-private-network-ip.

Module 07: Network Penetration Testing - Perimeter Devices

190. Nmap – Techniques for Avoiding Firewalls, last modified: 2012, https://pentestlab.blog/2012/04/02/nmap-techniques-for-avoiding-firewalls/.
191. Firewall Penetration Testing – Part II, last modified: 2017, https://www.provensec.com/firewall-penetration-testing-part-ii/.
192. Michael Gregg, Network security assessment: Test firewalls, IDS in multiple ways, accessed: January 11, 2018, http://searchnetworking.techtarget.com/tip/Network-security-assessment-Test-firewalls-IDS-in-multiple-ways.
193. Information Security Aficionado, last modified: 2014, https://infosecninja.blogspot.in/2014/05/m0n0wall-firewall-penetration-testing.html.
194. MountAraratBlossom, FIREWALL PENETRATION TESTING, last modified: 2000, http://taz.newffr.com/TAZ/Sysadm/firewall/FIREWALL%20PENETRATION%20TESTING.htm.
195. Murray Brand, A Comprehensive Firewall Testing Methodology, last modified: 2007, http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1021&context=ism.
196. Reto E. Haeni, Firewall Penetration Testing, last modified: 1997, http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.42.1117&rep=rep1&type=pdf.

197. Karen Scarfone, Paul Hoffman, Guidelines on Firewalls and Firewall Policy, last modified: 2009, https://csrc.nist.gov/publications/detail/sp/800-41/rev-1/final.
198. Hoon Ko, Special Issues for Penetration testing of Firew all, last modified: 2008, http://www.sersc.org/journals/JSE/vol5_no4_2008/5.pdf.
199. Firewalls, accessed: January 11, 2018, https://www.cs.columbia.edu/~smb/classes/f06/l15.pdf.
200. Avi Kak, Lecture 18: Packet Filtering Firewalls (Linux), last modified: 2017, https://engineering.purdue.edu/kak/compsec/NewLectures/Lecture18.pdf.
201. Adam Gowdiak, Techniques used for bypassing firewall systems, last modified: 2003, https://www.terena.org/activities/tf-csirt/meeting9/gowdiak-bypassing-firewalls.pdf.
202. A Penetration Testing Model, accessed: January 11, 2018, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Studies/Penetration/penetration_pdf.pdf?__blob=publicationFile.
203. Nathan House, Firewall Test Agent, last modified: 2005, https://www.stationx.net/firewall-test-agent/.
204. Nathan Einwechter, Multi-Layer Intrusion Detection Systems, last modified: 2004, https://www.symantec.com/connect/articles/multi-layer-intrusion-detection-systems.
205. David Del Elson, Focus On Linux: Intrusion Detection on Linux, last modified: 2000, https://www.symantec.com/connect/articles/focus-linux-intrusion-detection-linux.
206. Jamil Farshchi, Wireless Intrusion Detection Systems, last modified: 2003, https://www.symantec.com/connect/articles/wireless-intrusion-detection-systems.
207. Karen Scarfone, Peter Mell, Guide to Intrusion Detection and Prevention Systems (IDPS), last modified: 2007, https://csrc.nist.gov/publications/detail/sp/800-94/final.
208. Intrusion detection and penetration tests, accessed: January 11, 2018, http://www.gipsa-lab.grenoble-inp.fr/~jean-marc.thiriet/ipa/8-CourseIDS.pdf.
209. Stefan Zota, Intrusion Detection – Backscatter and Global Analysis, accessed: January 11, 2018, http://www.cs.unc.edu/~jeffay/courses/nidsS05/slides/14-Measurement.pdf.
210. Falko Timme, Securing Your Server With A Host-based Intrusion Detection System, accessed: January 11, 2018, https://www.howtoforge.com/intrusion_detection_with_ossec_hids.
211. iDefense Intelligence Operations Team, Intrusion Detection System (IDS) Evasion, last modified: 2006, http://complianceandprivacy.com/WhitePapers/iDefense-IDS-Evasion/iDefense_IDSEvasion_20060510.pdf.
212. Intrusion Detection System (IDS) Evasion Techniques, last modified: 2007, http://johncrackernet.blogspot.in/2007/01/intrusion-detection-system-ids-evasion.html.
213. Gerhard Zaugg, Firewall Testing, last modified: 2004, http://archiv.infsec.ethz.ch/education/projects/archive/Bericht_Gerry.pdf.
214. 8 Most Common IT Security Vulnerabilities And strategies for effective Penetration Testing, accessed: January 11, 2018, https://www.mti.com/wp-content/uploads/2017/08/MTI-Pen-Test-Guide.pdf.
215. Security Testing, last modified: 2016, https://assets.kpmg.com/content/dam/kpmg/ch/pdf/cyber-defense-services-security-testing-en.pdf.

Module 08: Web Application Penetration Testing

216. Secforce, Black box penetration testing vs white box penetration testing, last modified: 2008, https://www.secforce.com/blog/2008/11/black-box-penetration-testing-vs-white-box-penetration-testing/.
217. Attack Surface Analysis Cheat Sheet, last modified: 2017, https://www.owasp.org/index.php/Attack_Surface_Analysis_Cheat_Sheet.
218. Top 10 2007-Insecure Cryptographic Storage, accessed: January 12, 2018, https://www.owasp.org/index.php/Top_10_2007-Insecure_Cryptographic_Storage.
219. OWASP TESTING GUIDE, last modified: 2008, https://www.owasp.org/images/5/56/OWASP_Testing_Guide_v3.pdf.
220. Testing: Introduction and objectives, accessed: January 12, 2018, https://www.owasp.org/index.php/Testing:_Introduction_and_objectives.
221. Dafydd Stuttard and Marcus Pinto, The Web Application Hacker's Handbook, last modified: 2008, http://mimoza.marmara.edu.tr/~msakalli/cse711/The.Web.Application.Hackers.Handbook.Oct.2007.pdf.
222. Robert Auger, Fingerprinting, last modified: 2009, http://projects.webappsec.org/w/page/13246925/Fingerprinting.

223. Johnny Long, Google Hacking for Penetration Testers, accessed: January 12, 2018, https://www.blackhat.com/presentations/bh-europe-05/BH_EU_05-Long.pdf.

224. Don, Oracle Web Hacking Part II, last modified: 2011, https://www.ethicalhacker.net/columns/gates/oracle-web-hacking-part-ii.

225. Troy Giunipero, Creating a Simple Web Application Using a MySQL Database, accessed: January 12, 2018, https://netbeans.org/kb/docs/web/mysql-webapp.html.

226. Bruce Leban, Mugdha Bendre, and Parisa Tabriz, Web Application Exploits and Defenses, accessed: January 12, 2018, http://google-gruyere.appspot.com/.

227. Identify and classify potential threats to a system and describe how a given architecture will address the threats, accessed: January 12, 2018, http://java.boot.by/scea5-guide/ch08s03.html.

228. URL manipulation attacks, last modified: 2017, http://ccm.net/contents/31-url-manipulation-attacks.

229. Top 10 2007-Insecure Cryptographic Storage, accessed: January 12, 2018, https://www.owasp.org/index.php/Top_10_2007-Insecure_Cryptographic_Storage.

230. Andrey Petukhov, Dmitry Kozlov, Detecting Security Vulnerabilities in Web Applications Using Dynamic Analysis with Penetration Testing, last modified: 2008, https://www.owasp.org/images/3/3e/OWASP-AppSecEU08-Petukhov.pdf.

231. Jody Melbourne and David Jorm, Penetration Testing for Web Applications (Part One), last modified: 2003, http://www.it-docs.net/ddata/851.pdf.

232. Kunjan Shah, Penetration Testing for iPhone/iPad Applications, last modified: 2011, https://www.mcafee.com/in/resources/white-papers/foundstone/wp-pen-testing-iphone-ipad-apps.pdf.

233. Insecure Cryptographic Storage Explained, last modified: 2012, http://www.veracode.com/blog/2012/06/insecure-cryptographic-storage-explained.

234. Dr. E. Benoist, nsecure Cryptographic Storage, last modified: 2012, http://www.benoist.ch/WebSecurity/slides/insecureCryptoStorage/slidesInsecureCryptoStorage.pdf.

235. URL manipulation attacks, last modified: 2017, http://ccm.net/contents/31-url-manipulation-attacks.

236. Krzysztof Kotowicz, SQL Injection: complete walkthrough (not only) for PHP developers, last modified: 2010, http://www.slideshare.net/kkotowicz/sql-injection-complete-walktrough-not-only-for-php-developers.

237. Jumping Bean, SQL Injection Vulnerabilities and How to Prevent Them, last modified: 2015, https://www.slideshare.net/mxc4/sql-injectionvulnerabilitiesprevention.

238. Justin Clarke, SQL Injection Attacks and Defense, last modified: 2012, https://books.google.co.in/books?id=KKqiht2IsrcC&pg=PA29&lpg=PA29&dq=discovering+get+and+post++parameters+for+sql+injection&source=bl&ots=Cc9G4_4Jcq&sig=vbOSmeie1lI53blw2nnX6euoC5g&hl=en&sa=X&ei=z-9vVebpHIu2uASO7YHwAw&ved=0CFUQ6AEwCQ#v=onepage&q=discovering%20get%20and%20post%20%20parameters%20for%20sql%20injection&f=false.

239. Chad Dougherty, Practical Identification of SQL Injection Vulnerabilities, last modified: 2012, https://www.us-cert.gov/sites/default/files/publications/Practical-SQLi-Identification.pdf.

240. Ferruh Mavituna, DOS ATTACKS USING SQL WILDCARDS, accessed: January 12, 2018, https://labs.portcullis.co.uk/download/DoS_Attacks_Using_SQL_Wildcards.pdf.

241. How to Hack Databases: Extracting Data from Online Databases Using Sqlmap, last modified: 2014, https://null-byte.wonderhowto.com/how-to/hack-databases-extracting-data-from-online-databases-using-sqlmap-0150688/.

242. Procedural SQL injection, accessed: January 12, 2018, https://stormsecurity.wordpress.com/2008/10/15/procedural-sql-injection/.

243. Command Line Execution through SQL Injection, accessed: January 12, 2018, https://capec.mitre.org/data/definitions/108.html.

244. Basic Tests for SQL-Injection Vulnerabilities, last modified: 2015, http://www.joellipman.com/articles/web-development/503-basic-tests-for-sql-injection-vulnerabilities.html.

245. Bernardo Damele A. G., Advanced SQL injection to operating system full control, last modified: 2009, https://www.owasp.org/images/d/dc/AppsecEU09-Damele-A-G-Advanced-SQL-injection-slides.pdf.

246. Joe McCray, Advanced SQL Injection, accessed: January 12, 2018, https://defcon.org/images/defcon-17/dc-17-presentations/defcon-17-joseph_mccray-adv_sql_injection.pdf.

247. Bernardo Damele A. G., SQL injection: Not only AND 1=1, last modified: 2009, https://www.owasp.org/images/e/ed/SQLinjectionNotOnly.pdf.

248. DMITRY EVTEEV, A BACKDOOR IN THE NEXT GENERATION ACTIVE DIRECTORY, accessed: January 12, 2018, https://www.ptsecurity.com/upload/corporate/ww-en/download/A%20Backdoor%20in%20the%20Next%20Generation%20Active%20Directory_eng.pdf.

249. SQL Injection, accessed: January 12, 2018, https://www.owasp.org/index.php/SQL_Injection.

250. William G.J. Halfond, Jeremy Viegas, and Alessandro Orso, A Classification of SQL Injection Attacks and Countermeasures, last modified: 2006, http://www.cc.gatech.edu/fac/Alex.Orso/papers/halfond.viegas.orso.ISSSE06.pdf.

251. Joseph Muniz, Aamir Lakhani, Web Penetration Testing with Kali Linux, last modified: 2013, ftp://lab.dnict.vn/1.DNICT/2.Ebooks/books/Web%20Penetration%20Testing%20with%20Kali%20Linux.pdf.

252. Dafydd Stuttard Marcus Pinto, The Web Application Hacker's Handbook, last modified: 2011, https://leaksource.files.wordpress.com/2014/08/the-web-application-hackers-handbook.pdf.

253. Web Application Penetrating Testing Methodology, accessed: January 12, 2018, http://resources.infosecinstitute.com/wp-content/uploads/Web-Application-Penetrating-Testing-Methodology.pdf.

254. Georgia Weidman, Penetration testing A Hands-On Introduction to Hacking, last modified: 2014, https://repo.zenk-security.com/Magazine%20E-book/Penetration%20Testing%20-%20A%20hands-on%20introduction%20to%20Hacking.pdf.

255. Security Testing, last modified: 2016, https://assets.kpmg.com/content/dam/kpmg/ch/pdf/cyber-defense-services-security-testing-en.pdf.

256. RAFAY BALOCH, ETHICAL HACKING AND PENETRATION TESTING GUIDE, last modified: 2015, http://www.ittoday.info/Excerpts/Postexploitation.pdf.

Module 09: Wireless Penetration Testing

257. Satish b, Penetration testing of iPhone Applications – Part 4, last modified: 2013, http://www.securitylearn.net/tag/iphone-snapshot-storage/.

258. Satish b, Hacking and securing ios applications, last modified: 2012, https://www.slideshare.net/securitylearnwordpress/hacking-and-securing-ios-applications.

259. Max Veytsman & Subu Ramanathan, Deep Dive: PenTesting the Android and iPhone, last modified: 2011, https://www.securitycompass.com/conferences/downloads/pentesting_android_iphone.pdf.

260. WIRELESS NETWORK SECURITY, last modified: 2003, http://www.antenna.com/Proxim%20Wireless%20Security.pdf.

261. Paul Asadoorian, Wireless Network Security?, accessed: January 8, 2018, https://securityweekly.com/WirelessNetSec.pdf.

262. Wireless LAN Security, accessed: January 8, 2018, https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/wireless-LAN-security-02-en.pdf.

263. WIRELESS NETWORKING SECURITY, last modified: 2010, https://www.infosec.gov.hk/english/technical/files/wireless.pdf.

264. Rogue Access Point Detection, accessed: January 8, 2018, https://www.watchguard.com/help/docs/fireware/12/en-US/Content/en-US/wireless/wireless_rogue_ap_detection_c.html.

265. Sgt. Christopher Then, Examining Wireless Access Points and Associated Devices, last modified: 2006, http://www.forensicfocus.com/downloads/examining-wireless-access-points.pdf.

266. Jonathan Hassell, Wireless Attacks and Penetration Testing (part 2 of 3), last modified: 2004, https://www.symantec.com/connect/articles/wireless-attacks-and-penetration-testing-part-2-3.

267. Michael Ossmann, WEP: Dead Again, Part 2, last modified: 2005, https://www.symantec.com/connect/articles/wep-dead-again-part-2.

Module 10: IoT Penetration Testing

268. Bus Pirate, last modified: October 2019, http://dangerousprototypes.com/docs/Bus_Pirate.

269. FIRMADYNE, last modified: 2020, https://github.com/firmadyne/firmadyne.

270. Firmware Analysis Toolkit, last modified: 2020, https://github.com/attify/firmware-analysis-toolkit.

Module 11: OT and SCADA Penetration Testing

271. Arping, last modified: 2020, https://github.com/ThomasHabets/arping.

272. Iputils, last modified: 2020, https://github.com/ThomasHabets/arping.

273. Use arp-scan to find hidden devices in your network, last modified: 2015, https://github.com/iputils/iputils.

274. OUI Lookup Tool, https://www.wireshark.org/tools/oui-lookup.html.

275. GRASSMARLIN, last modified: 2017, https://github.com/nsacyber/GRASSMARLIN.

Module 12: Cloud Penetration Testing

276. Rob Shapland, AWS penetration testing secrets for success, last modified: 2015, http://searchcloudsecurity.techtarget.com/tip/AWS-penetration-testing-secrets-for-success.

277. Frank Siemons, Penetration Testing and Cloud Platforms, accessed: January 5, 2018, http://resources.infosecinstitute.com/penetration-testing-and-cloud-platforms/#gref.

278. Pen testing cloud-based apps: A step-by-step guide, accessed: January 5, 2018, https://techbeacon.com/pen-testing-cloud-based-apps-step-step-guide.

279. BALAJI N, Cloud Computing Penetration Testing Checklist & Important Considerations, last modified: 2017, https://gbhackers.com/cloud-computing-penetration-testing-checklist-important-considerations/#.

280. Pen Testing, last modified: 2017, https://docs.microsoft.com/en-us/azure/security/azure-security-pen-testing.

281. Microsoft Cloud Unified Penetration Testing Rules of Engagement, accessed: January 5, 2018, https://technet.microsoft.com/en-us/mt784683.

282. Penetration Testing, accessed: January 5, 2018, https://aws.amazon.com/security/penetration-testing/.

283. Submit Azure Service Penetration Testing Notification, accessed: January 5, 2018, https://portal.msrc.microsoft.com/en-us/engage/pentest.

284. GOOGLE CLOUD PLATFORM SECURITY, accessed: January 5, 2018, https://cloud.google.com/security/.

285. QuoteColo, Cloud Computing in 2014: Facts and Predictions, last modified: 2014, http://www.quotecolo.com/cloud-computing-in-2014-facts-and-predictions-infographic/.

286. Louis Columbus, Gartner Predicts Infrastructure Services Will Accelerate Cloud Computing Growth, last modified: 2013, https://www.forbes.com/sites/louiscolumbus/2013/02/19/gartner-predicts-infrastructure-services-will-accelerate-cloud-computing-growth/#f96c18c1938c.

287. Cloud Computing Vulnerability Incidents: A Statistical Overview, accessed: January 5, 2018, https://cloudsecurityalliance.org/download/cloud-computing-vulnerability-incidents-a-statistical-overview/.

288. Introduction to Cloud Computing, last modified: 2013, https://www.slideshare.net/ProfEdge/introduction-to-cloud-computing-23970527.

289. Kazi Zunnurhain and Susan V. Vrbsky, Security Attacks and Solutions in Clouds, accessed: January 5, 2018, http://salsahpc.indiana.edu/CloudCom2010/Poster/cloudcom2010_submission_98.pdf.

290. Chimere Barron, Huiming Yu and Justin Zhan, Cloud Computing Security Case Studies and Research, last modified: 2013, http://www.iaeng.org/publication/WCE2013/WCE2013_pp1287-1291.pdf.

291. Keiko Hashizume, David G Rosado, Eduardo Fernández-Medina and Eduardo B Fernandez, An analysis of security issues for cloud computing, last modified: 2013, https://jisajournal.springeropen.com/articles/10.1186/1869-0238-4-5.

292. SECURITY GUIDANCE FOR CRITICAL AREAS OF FOCUS IN CLOUD COMPUTING V3.0, last modified: 2011, https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf.

293. Cloud Computing in 2014: Facts and Predictions (Infographic), last modified: 2014, http://www.quotecolo.com/cloud-computing-in-2014-facts-and-predictions-infographic/.

294. Jonathan Edwards, Why are More and More Businesses Moving to the Cloud?, last modified: 2012, http://www.yorkshirecloud.co.uk/more-businesses-moving-to-cloud-computing/.

295. Louis Columbus, Gartner Predicts Infrastructure Services Will Accelerate Cloud Computing Growth, last modified: 2013, http://www.forbes.com/sites/louiscolumbus/2013/02/19/gartner-predicts-infrastructure-services-will-accelerate-cloud-computing-growth/.

296. Cloud Computing Vulnerability Incidents: A Statistical Overview, accessed: January 5, 2018, https://cloudsecurityalliance.org/download/cloud-computing-vulnerability-incidents-a-statistical-overview/.

297. Introduction to Cloud Computing, last modified: 2013, http://www.slideshare.net/ProfEdge/introduction-to-cloud-computing-23970527.

298. Kazi Zunnurhain and Susan V. Vrbsky, Security Attacks and Solutions in Clouds, accessed: January 5, 2018, http://salsahpc.indiana.edu/CloudCom2010/Poster/cloudcom2010_submission_98.pdf.

299. Chimere Barron, Huiming Yu and Justin Zhan, Cloud Computing Security Case Studies and Research, last modified: 2013, http://www.iaeng.org/publication/WCE2013/WCE2013_pp1287-1291.pdf.

300. An analysis of security issues for cloud computing, last modified: 2013, https://jisajournal.springeropen.com/articles/10.1186/1869-0238-4-5.

301. Security Assessments, last modified: 2012, https://downloads.cloudsecurityalliance.org/initiatives/secaas/SecaaS_Cat_5_Security_Assessments_Implementation_Guidance.pdf.

302. A Briefing on Cloud Security Challenges and Opportunities, last modified: 2013, https://www.telenor.com/wp-content/uploads/2013/11/TelenorWhitepaperCloud-V_30_v.pdf.

303. Cloud Computing Information Security and Privacy Considerations, last modified: 2014, https://www.ict.govt.nz/assets/ICT-System-Assurance/Cloud-Computing-Information-Security-and-Privacy-Considerations-FINAL2.pdf.

304. Introduction to AWS Security, last modified: 2015, http://www.cloud9infosystems.com/pdf/AWS_Security.pdf.

305. Google Security Whitepaper, accessed: January 5, 2018, https://www.screenleap.com/doc/Google_Cloud_Platform_Security_Whitepaper.pdf.

306. Amazon AWS Penetration Testing, last modified: 2020, https://www.packetlabs.net/amazon-aws-penetration-testing/.

307. Spencer Gietzen, AWS IAM Privilege Escalation – Methods and Mitigation, https://rhinosecuritylabs.com/aws/aws-privilege-escalation-methods-mitigation/.

308. Versioning IAM policies, https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_managed-versioning.html.

309. create-policy, https://awscli.amazonaws.com/v2/documentation/api/latest/reference/iam/create-policy.html.

310. set-default-policy-version, https://awscli.amazonaws.com/v2/documentation/api/latest/reference/iam/set-default-policy-version.html.

311. IAM roles for Amazon EC2, https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/iam-roles-for-amazon-ec2.html.

312. create-access-key, https://awscli.amazonaws.com/v2/documentation/api/latest/reference/iam/create-access-key.html.

313. create-login-profile, https://awscli.amazonaws.com/v2/documentation/api/latest/reference/iam/create-login-profile.html.

314. update-login-profile, https://awscli.amazonaws.com/v2/documentation/api/latest/reference/iam/update-login-profile.html.

315. attach-user-policy, https://awscli.amazonaws.com/v2/documentation/api/latest/reference/iam/attach-user-policy.html.

316. attach-group-policy, https://awscli.amazonaws.com/v2/documentation/api/latest/reference/iam/attach-group-policy.html.

317. attach-role-policy, https://awscli.amazonaws.com/v2/documentation/api/latest/reference/iam/attach-role-policy.html.

318. put-user-policy, https://awscli.amazonaws.com/v2/documentation/api/latest/reference/iam/put-user-policy.html.

319. put-group-policy, https://awscli.amazonaws.com/v2/documentation/api/latest/reference/iam/put-group-policy.html.

320. put-role-policy, https://awscli.amazonaws.com/v2/documentation/api/latest/reference/iam/put-role-policy.html.

321. add-user-to-group, https://awscli.amazonaws.com/v2/documentation/api/latest/reference/iam/add-user-to-group.html.

322. update-assume-role-policy, https://awscli.amazonaws.com/v2/documentation/api/latest/reference/iam/update-assume-role-policy.html.

323. Penetration testing, last modified: August 8, 2020, https://docs.microsoft.com/en-us/azure/security/fundamentals/pen-testing.

324. Penetration Testing Rules of Engagement, https://www.microsoft.com/en-us/msrc/pentest-rules-of-engagement?rtc=1.

325. Yuri Diogenes, Dr. Thomas W. Shinder, Microsoft Azure Security Center, https://cdn.ttgtmedia.com/rms/pdf/MSazuresec_ch4.pdf.

326. THE 10 MOST COMMON AZURE MISCONFIGURATIONS AND HOW TO FIX THEM, http://click.cloudcheckr.com/rs/222-ENM-584/images/Azure-Misconfigurations-WP-V4.pdf.

327. THE 7 DEADLY SINS OF AZURE MISCONFIGURATION AND HOW TO FIX THEM, https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE36QLE.

328. Adil Arif, Implement Storage Encryption, last modified: February 20, 2018, https://www.enterprisedaddy.com/2018/02/objective-3-4-implement-storage-encryption/.

329. Configuring retention in Azure Time Series Insights Gen1, last modified: June 30, 2020, https://docs.microsoft.com/en-us/azure/time-series-insights/time-series-insights-how-to-configure-retention.

330. Enable JIT VM access, last modified: July 12, 2020, https://docs.microsoft.com/en-us/azure/security-center/security-center-just-in-time?tabs=jit-config-avm%2Cjit-request-asc#enable-jit-vm-access-.

331. Just-in-time (JIT) VM access for Azure Firewall is now generally available, last modified: 21 August, 2019, https://azure.microsoft.com/en-in/updates/just-in-time-jit-vm-access-for-azure-firewall-is-now-generally-available/.
332. Cloud Security FAQ, https://support.google.com/cloud/answer/6262505?hl=en.
333. Take command of your security in the cloud, last modified: December 2019, https://services.google.com/fh/files/misc/wp_take_command_of_your_security_in_the_cloud_rgb_v15c.pdf.
334. Using Container Threat Detection, last modified: September 9, 2020, https://cloud.google.com/security-command-center/docs/how-to-use-container-threat-detection.
335. Setting up Security Command Center, last modified: September 18, 2020, https://cloud.google.com/security-command-center/docs/quickstart-security-command-center.

Module 13: Binary Analysis and Exploitation

336. Intel® 64 and IA-32 Architectures Software Developer's Manual, last modified: October 2019, https://software.intel.com/sites/default/files/managed/39/c5/325462-sdm-vol-1-2abcd-3abcd.pdf
337. NASM – The Netwide Assembler, https://www.nasm.us/xdoc/2.14.02/nasmdoc.pdf.
338. Tool Interface Standard (TIS) Executable and Linking Format (ELF) Specification http://refspecs.linuxbase.org/elf/elf.pdf
339. x86-64, last modified: September 29, 2020, https://en.wikipedia.org/wiki/X86-64

Module 14: Report Writing and Post Testing Actions

340. Penetration Testing Report, accessed: January 5, 2018, http://www.niiconsulting.com/services/security-assessment/NII_Sample_PT_Report.pdf.
341. Penetration Test Report, last modified: 2013, http://www.offensive-security.com/penetration-testing-sample-report.pdf.
342. John Smith, DOCUMENTATION FORMS FOR PENETRATION TESTS, last modified: 2003, http://www.delmarlearning.com/companions/content/1435486099/documents/Documentation_Forms.pdf.
343. Matt Dobinson, Penetration Testing & Deep Code Analyst Report, last modified: 2011, https://www.slideshare.net/SanjulikaRastogi/penetration-security-testing.
344. Karen Scarfone (NIST), Murugiah Souppaya (NIST), Amanda Cody (BAH), Angela Orebaugh (BAH), Technical Guide to Information Security Testing and Assessment, last modified: 2008, http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf.
345. Information Supplement: Penetration Testing Guidance, last modified: 2015, https://www.pcisecuritystandards.org/documents/Penetration_Testing_Guidance_March_2015.pdf.
346. Kevin Orrey, Vulnerabilityassessment.co.uk, accessed: January 5, 2018, http://www.vulnerabilityassessment.co.uk/report%20template.html.
347. Benjamin Caudill, Four Things Every Penetration Test Report Should Have, from https://rhinosecuritylabs.com/penetration-testing/four-things-every-penetration-test-report/.
348. Semi Yulianto, (2019), Tutorial: Writing An Effective Penetration Testing Report, from https://www.youtube.com/watch?v=OKN5pUgQKIM.
349. (2019), Writing a Pentest Report, from https://www.youtube.com/watch?v=EOoBAq6z4Zk.
350. Kevin Johnson, (2019), What is an Attestation Letter?, from https://secureideas.com/knowledge/what-is-a-letter-of-attestation.
351. Penetration Testing Overview, from https://alpinesecurity.com/services/penetration-testing-overview/.